AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (currently amended) A security system for repelling viruses in computers and computer networks~~, which security system~~ and that is adapted to forward messages, ~~characterized in that~~ the security system ~~includes~~ comprising a first sub-system (1) to detect unknown viruses, ~~which~~ said first sub-system ~~(1) is~~ being adapted in connection with the forwarding of messages or with other action or, in a timed manner, to perform ~~at least one action~~ one or more predetermined actions to activate unknown viruses and to detect the activated unknown viruses by detecting consequences of virus activation.

2. (currently amended) [[A]] The security system in accordance with Claim 1, ~~characterized in that it is~~ that is adapted to forward an alarm caused by the detection of a virus to at least one system connected to the security system [[(2,3)]].

3. (currently amended) [[A]] The security system in accordance with Claim 1, ~~characterized in that it is~~ that is further adapted to break ~~the~~ a connection to at least one other system ~~(2,3, 114)~~ on the basis of an alarm caused by the detection of a virus.

4. (currently amended) [[A]] The security system in accordance with Claim 1, ~~characterized in that it additionally includes~~ further comprising a second sub-system [[(2)]] for forwarding messages from the first sub-system [[(1)]] to at least one system ~~(3, 210, 114)~~ connected to the security system.

5. (currently amended) [[A]] The security system in accordance with Claim 1, ~~characterized in that it additionally includes~~ further comprising a third sub-system [[(3)]] that is adapted to break ~~the~~ a connection to at least one other sub-system ~~(1,2)~~ upon receiving an alarm.

6. (currently amended) [[A]] The security system in accordance with Claim 5, ~~characterized in that~~ wherein the ~~second~~ at least one other sub-system [[(2)]] includes an identifier which corresponds to an identifier of ~~the apparatus (3) of~~ the third sub-system.

7. (canceled)

8. (currently amended) [[A]] The security system in accordance with Claim 2, ~~characterized in that~~ wherein the alarm is a message or at least a part of a message that is forwarded to the recipient quicker than other communications.

9. (currently amended) [[A]] The security system in accordance with Claim 5, ~~characterized in that~~ wherein the third sub-system [[(3)]] includes at least one computer or one network element including a computer.

10. (currently amended) [[A]] The security system in accordance with Claim 2, ~~characterized in that~~ wherein the alarm is forwarded via a separate connection.

11. (currently amended) [[A]] The security system in accordance with Claim 1, ~~characterized in that the said action is one the following:~~ wherein the one or more predetermined actions include at least one of altering the time data, altering the contents of the memory, handling of files or at least its partial simulation.

12. (currently amended) [[A]] The security system in accordance with Claim 1, ~~characterized in that it is adapted to detect an activated virus when at least one of the following conditions is met~~ wherein the consequences of virus activation detected by the first sub-system include at least one of: a change takes place in the first sub-system [[(1)]] prior to actions causing changes carried out by the ~~first-mentioned~~ first sub-system, a change takes place in the first sub-system [[(1)]] that is not an action taken by the ~~said~~ first sub-system to detect a virus, a message leaves for another system without command from the first sub-system [[(1)]], a message leaves for another system to a wrong address or to a system which no communication has been directed to, and a message does not leave for another system although it has been sent there.

13. (currently amended) [[A]] The security system in accordance with Claim 1, ~~characterized in that it is adapted to~~

~~combine activation measures of viruses to~~ wherein the one or more predetermined actions include plural actions that take place either simultaneously or consecutively in time.

14. (currently amended) [[A]] The security system in accordance with Claim 1, ~~characterized in that it~~ wherein the first sub-system is adapted to choose one or more of the following logics when trying to activate viruses: one defined by the user, pre-programmed or at least partially random logic.

15. (currently amended) [[A]] The security system in accordance with Claim 5, ~~characterized in that to it has been connected parallel with a third sub-system (3)~~ further comprising a parallel system that is adapted to save a message sent from the third sub-system [[(3)]], the parallel system being connected in parallel with the third sub-system.

16. (currently amended) [[A]] The security system in accordance with Claim 15, ~~characterized in that~~ wherein the first sub-system [[(1)]] is adapted to compare in [[a]] the parallel system a message sent from the third sub-system [[(3)]] to the first sub-system [[(1)]] and additionally saved in the parallel system in order to detect an anomaly caused by a virus.

17. (currently amended) [[A]] The security system in accordance with Claim 15, ~~characterized in that the above-mentioned~~ wherein the parallel system is adapted to forward a message saved by it.

18. (currently amended) [[A]] The security system in accordance with Claim 1, ~~characterized in that it is~~ that is adapted to examine messages forwarded through [[it]] the security system in order to detect known viruses.

19. (currently amended) [[A]] The security system in accordance with Claim 4, ~~characterized in that in order to isolate data between the first (114) and the second (3) system, it has been~~ comprising first and second ones of the at least one system, wherein the security system is adapted to transfer data between the first [[(114)]] and the second [[(3)]] ones of the at least one system through the first [[(1)]] and the second ~~(2) sub-system, which~~ sub-systems, and wherein the security system is adapted to disrupt the connection between the first one of the at least one system [[(114)]] and the first [[(1)]] sub-system before a connection is established between the first [[(1)]] and the second ~~(2) sub-system,~~ sub-systems and ~~is adapted~~ to disrupt the connection between the first [[(1)]] and the second ~~(2) sub-system~~ sub-systems before a connection is established between the second sub-system [[(2)]] and the second one of the at least one system [[(3)]].

20. (currently amended) ~~A security system for repelling viruses in computers and computer networks, which security system is adapted to forward messages, characterized in that the security system includes a first sub-system (1) for detecting unknown viruses, which~~ The security system in

accordance with claim 1, wherein said first sub-system [[(1)]] is adapted to compare messages with at least partially identical identifiers with each other in order to detect unknown viruses.

21. (currently amended) [[A]] The security system in accordance with Claim 20, ~~characterized in that it~~ wherein the first sub-system is adapted to request the sender of the ~~above-mentioned~~ messages with ~~the same~~ at least partially identical identifiers to re-send at least one ~~message with the same identifier~~ of the messages and is further adapted to compare at least one re-sent message received with the ~~above-mentioned~~ original messages in order to detect messages containing viruses.

22. (currently amended) A method for repelling viruses in computers and data networks, ~~characterized in that it is~~ the method being carried out in a security system including a first sub-system [[(1)]] for forwarding messages and for detecting viruses~~, which first sub-system (1) can, with regard to data transfer, be isolated from the rest of the system, which~~ and that is isolatable from a remainder of the security system, the method includes the steps where:

- [[the]] functions of the security system are monitored by the first sub-system in order to detect [[a]] consequences of activation of an unknown virus [[(311)]], ~~a virus (312) is detected when~~ the consequences of activation including at least one of the following ~~conditions are met~~: a change takes place in the first sub-system [[(1)]] prior to

actions causing changes carried out by the ~~first-mentioned~~ first sub-system, a change takes place in the first sub-system [[(1)]] that is not an action taken by the ~~said~~ first sub-system to detect a virus, a message leaves for another system without command from the first sub- system [[(1)]], a message leaves for another system to a wrong address or to a system which no communication has been directed to, and a message does not leave for another system although it has been sent there,

- a virus is detected when one of the consequences is detected, and

- an alarm [[(316)]] is given.

23. (currently amended) A method for repelling viruses in computers and computer networks, ~~characterized in that~~ the method ~~has stages where~~ comprising the steps of:

~~- at least one action in the system is taken~~ taking one or more predetermined actions to activate unknown viruses in connection with the forwarding of messages or other action, or in a timed manner~~, in order to activate a virus (310)~~,

~~- the actions of the system are monitored in order to detect an occurrence initiated by virus activation (311)~~ detecting the activated unknown viruses by detecting consequences of virus activation caused by the one or more predetermined actions, and

[[-]] giving an alarm ~~(316) is given~~ when a virus is detected [[(312)]].

24. (canceled)

25. (currently amended) [[A]] The method in accordance with Claim 23, ~~characterized in that the action taken to activate a virus is~~ wherein the one or more predetermined actions include at least one of the following: altering the time data, altering the contents of the memory, handling of files or at least its partial simulation.

26. (currently amended) [[A]] The method in accordance with Claim 23, ~~characterized in that it~~ wherein the method is run in a security system including a first sub-system [[(1)]] and a second sub-system ~~(2) in which method the activation of a virus is detected when at least one of the following conditions is met~~ and wherein the consequences of virus activation include at least one of: a change takes place in the first sub-system [[(1)]] prior to actions causing changes carried out by the ~~first-mentioned~~ first sub-system, a change takes place in the first sub-system [[(1)]] that is not an action taken by the ~~said~~ first sub-system to detect a virus, a message leaves for another system without command from the first sub-system [[(1)]], a message leaves for another system to a wrong address or to a system which no communication has been directed to, and a message does not leave for another system although it has been sent there.

27. (currently amended) [[A]] The method in accordance with Claim 23, ~~characterized in that in order to activate a virus, activation measures are combined to~~ wherein the one or

more predetermined actions include plural actions that take place either simultaneously or consecutively in time.

28. (currently amended) [[A]] The method in accordance with Claim 23, ~~characterized in that the~~ wherein the one or more predetermined actions include a logic ~~to be used when trying to activate a virus~~ that is one of the following: one defined by the user, pre-programmed or at least partially random logic.

29. (currently amended) [[A]] The method in accordance with Claim 23, ~~characterized in that it also includes a stage~~ further comprising the step where known viruses [[(306)]] are searched for on the basis of their characteristics.

30. (currently amended) [[A]] The method in accordance with Claim [[23]] 26, ~~characterized in that in order to isolate data~~ wherein the security system is connected to a first system and a second system and wherein data are transferred between the first system [[(114)]] and the second [[(3)]] system ~~the method is run in a security system that includes a~~ through the first sub-system [[(1)]] and [[a]] the second [[(2)]] sub-system ~~through which sub-systems (1,2) data is transferred between the first (114) and the second (3) system~~ phase by phase in order, in which phases:

- the connection for data transfer is disrupted between the first system [[(114)]] and the first sub-system [[(1)]],

- a connection for data transfer is established between the first sub-system [[(1)]] and the second sub-system [[(2)]],

- the connection for data transfer is disrupted between the first sub-system [[(1)]] and the second sub-system [[(2)]],

- a connection for data transfer is established between the second sub-system [[(2)]] and the second system [[(3)]].

31. (currently amended) An apparatus for repelling viruses in computers and computer networks, ~~which apparatus includes~~ comprising equipment for saving data ~~(610,612)~~ and for handling data [[(614)]] and equipment for transferring data [[(608)]] with another apparatus, ~~characterized in that~~ wherein the apparatus is adapted to receive a message ~~from the said other apparatus~~ and to perform ~~at least one action~~ one or more predetermined actions to activate unknown viruses contained in the message and to detect the activated unknown viruses by detecting consequences of virus activation.

32. (currently amended) [[An]] The apparatus in accordance with Claim 31, ~~characterized in that the action mentioned is~~ wherein the one or more predetermined actions include at least one of the following: altering the time data, altering the contents of the memory, handling of files or at least its partial simulation.

33. (currently amended) [[An]] The apparatus in accordance with Claim 31, ~~characterized in that it is adapted to detect virus activation when at least one of the following conditions is met~~ wherein the consequences of virus activation include at least one of: a change takes place prior to actions

caused by changes made by the apparatus, a change takes place that is not an action taken by the apparatus to detect a virus.

34. (currently amended) [[An]] The apparatus in accordance with Claim 31, ~~characterized in that it~~ wherein the apparatus is adapted to send a message to either a sub-assembly of the apparatus or to ~~the other~~ said another apparatus ~~mentioned~~, and ~~it is adapted to detect virus activation when at least one of the following conditions is met~~ wherein the consequences of virus activation include at least one of: a message leaves without authorization from the anti-virus software of the apparatus, a message leaves for an address it has not originally been directed to, a message does not leave although it has been given a command to be sent.

35. (currently amended) [[An]] The apparatus in accordance with Claim 31, ~~characterized in that it is adapted to combine virus activation measures to~~ wherein the one or more predetermined actions include plural actions that take place either simultaneously or consecutively in time.

36. (currently amended) [[An]] The apparatus in accordance with Claim 31, ~~characterized in that it is adapted to choose as the logic to be used when trying to activate a virus~~ wherein the one or more predetermined actions include a logic that is at least one of the following: one defined by the user, pre-programmed or at least partially random logic.

37. (currently amended) [[An]] The apparatus in accordance with Claim 31, ~~characterized in that it is adapted to examine~~ wherein the apparatus examines the message ~~mentioned~~ in order to detect known viruses.

38. (canceled)